

UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina ☐

In the Matter of the Seizure of)
(Briefly describe the property to be seized))
All cryptocurrency Tether held in address)
0xFa05456F82a0B816CD1dc1e9233BE75908fCd9b8)
)

Case No. 1:24MJ

387

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Middle District of North Carolina is subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(A) & (C) (describe the property):
982(a)(7)

All cryptocurrency Tether held in address 0xFa05456F82a0B816CD1dc1e9233BE75908fCd9b8

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

In accordance with Rule 4.1(b)(2)(A), the Applicant appeared before me by telephone, was placed under oath, and attested to the contents of this Application, which was submitted to me by reliable electronic means.

Attested by telephone CPA
Sworn to before me and signed in my presence.

Date: 10/03/24

City and state: Greensboro, North Carolina

/s/ David Yu

Applicant's signature

David Yu, Special Agent, FBI

Printed name and title

[Signature]
Judge's signature

Hon. L. Patrick Auld, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEIZURE WARRANTS

I, David Yu, Special Agent with the Federal Bureau of Investigation (“FBI”) state under penalty of perjury, pursuant to Title 28, United States Code, Section 1746, that the following is true and correct:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since January 1999. I am currently assigned to a criminal investigations squad of the Charlotte Division where my duties include the investigation of matters involving health care fraud.

2. I make this affidavit in support of applications for seizure warrants for the equivalent value of Tether (USDT) (the “**Subject Funds**”) stored in the following virtual currency addresses (the “**Subject Addresses**”):

a. All Tether (“USDT”) held in address

0xFa05456F82a0B816CD1dc1e9233BE75908fCd9b8 (“**Subject Address 1**”)

b. All Tether (“USDT”) held in address

0xD4C06e5554a2c4F18269126Cc5d530dd1D43dC4E (“**Subject Address 2**”)

The particular items to be seized are described in the following paragraphs and in Attachment A.

3. As further described below, this affidavit is made in support of applications for seizure warrants for funds traceable to, and involved in, a health care fraud scheme for which payments were subsequently laundered into the **Subject Addresses**.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that Chaudhry Ahmed, through at least two of his durable medical equipment companies, Dune Medical Supply, LLC and Prospect Health

Solutions, Inc., has violated 18 U.S.C. § 1347 (health care fraud) and laundered the proceeds of that activity in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and 18 U.S.C. § 1957 (money laundering and violation of the spending statute).

5. There is also probable cause to believe that the **Subject Addresses** received the proceeds of the health care fraud scheme described below and that the **Subject Funds** are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c). Moreover, there is probable cause to believe that the **Subject Funds** are subject to forfeiture as property involved in money laundering offenses, pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1).

6. The facts and information contained in this Affidavit are based on my personal knowledge, as well as information obtained from witness interviews, documents, law enforcement records, and information provided by other law enforcement officials, as well as other investigators and people involved in this investigation.

Statutory Authority

7. Health care fraud: 18 U.S.C. § 1347 prohibits (a) knowingly and willfully executing, or attempting to execute, a scheme or artifice (1) to defraud any health care benefit program; or (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program. A violation of Section 1347 is a “Federal health care offense” pursuant to 18 U.S.C. § 24(a).

- a. 18 U.S.C. § 24(b) defines a “health care benefit program” as “any public or private plan or contract, affecting commerce, under which any medical benefit, item, or service is provided to any individual, and includes any individual or entity who is providing a medical benefit, item, or service for which payment

may be made under the plan or contract.” Insurance companies that provide payment and reimbursement for medical services qualify as a health care benefit program. Medicare is a health care benefit program.

8. Concealment money laundering: 18 U.S.C. § 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

9. The Spending Statute: 18 U.S.C. § 1957 provides in relevant part that “[w]hoever . . . knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from specified unlawful activity” shall be guilty of a federal offense. Because the offense consists of spending the proceeds of specified unlawful activity, § 1957 is sometimes referred to as the Spending Statute. Violations of § 1957 are considered money laundering offenses.

10. The proceeds of health care fraud are subject to forfeiture under both civil and criminal forfeiture authorities. Pursuant to 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to health care fraud is subject to civil forfeiture. In addition, 28 U.S.C. § 2461(c) provides that, “[i]f a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized,” then the government can obtain forfeiture of property “as part of the sentence in the criminal case.” Thus, pursuant to 28 U.S.C. § 2461(c) and 18 U.S.C. § 981(a)(1)(C), any property,

real or personal, which constitutes or is derived from proceeds traceable to health care fraud is subject to criminal forfeiture.

11. Property involved in a money laundering offense is subject to forfeiture under both civil and criminal forfeiture authorities. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 or 1957, or any property traceable to such property, is subject to civil forfeiture. In addition, pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in a violation of 18 U.S.C. §§ 1956 or 1957, or any property traceable to such property, is subject to criminal forfeiture. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. Forfeitures encompass all property “involved in” the crime, which can include untainted funds that are comingled with tainted funds derived from illicit sources. *See United States v. Kivanc*, 714 F.3d 782, 794-95 (4th Cir. 2013) (“Consequently, when legitimate funds are comingled with property involved in money laundering or purchased with criminally derived proceeds, the entire property, including the legitimate funds, is subject to forfeiture.”).

12. This application seeks a seizure warrant under both civil and criminal authority, because the property to be seized could easily be placed beyond process if not seized by warrant, as virtual currency is fungible and easily dissipated.

13. 18 U.S.C. § 981(b) states that property subject to forfeiture under Section 981 may be seized via a civil seizure warrant issued by a judicial officer “in any district in which a forfeiture action against the property may be filed,” and may be executed “in any district in which the property is found,” if there is probable cause to believe the property is subject to forfeiture. 18 U.S.C. § 982(b)(1) incorporates the procedures in 21 U.S.C. § 853 (other than subsection (d)) for

all stages of a criminal forfeiture proceeding. Title 21 U.S.C. § 853(f) permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture.

BACKGROUND ON VIRTUAL CURRENCY

14. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin (“BTC”) is the most well-known virtual currency in use.

15. Virtual currency addresses are the specific virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters. Each virtual currency address is controlled through a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address’s private key can authorize a transfer of virtual currency from that address to another address.

16. Many virtual currencies publicly record their transactions on what is referred to as the “blockchain.” The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain’s specific technology. The blockchain can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

17. Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law

enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open-source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

18. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

19. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

20. Virtual currency exchanges are online platforms which allow individuals to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many virtual currency exchanges also store their customers' virtual currency addresses in hosted wallets, and such exchanges are often referred to as "custodial." Coinbase is an example of a U.S.-based custodial exchange.

21. USDT (also known as Tether) is a virtual currency that resides on multiple blockchains. USDT is hosted on the Ethereum and Tron blockchains, among others. USDT is a

stablecoin. Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens. The value of USDT is pegged to the value of the U.S. dollar.

22. Because Tether manages the smart contracts for USDT, it is able to freeze some addresses containing USDT. For example, as is relevant to this application, Tether is able to blacklist addresses on the Ethereum network, rendering them inaccessible to whomever controls the private keys to the frozen addresses. In the instant case, at the request of law enforcement, Tether voluntarily acted to freeze the USDT associated with the **Subject Addresses**. While USDT cannot be transferred from a frozen USDT address, USDT can still be transferred into a frozen address.

JURISDICTION AND VENUE

23. As explained in further detail below, seizures are appropriate from this district pursuant to 18 U.S.C. 981(b)(3) and 28 U.S.C. § 1355(b)(1), because it is a district in which any of the acts or omissions giving rise to the forfeiture occurred.

PROBABLE CAUSE OF HEALTH CARE FRAUD SCHEME

A. Background on Medicare and DME

24. The Medicare Program is a federally funded health insurance program for eligible persons 65 years of age and older, and certain disabled persons, under which physicians, hospitals and other health care providers are compensated or reimbursed for covered medical services and

supplies provided to Medicare beneficiaries. Medicare is a health care benefit program affecting commerce, as defined by Title 18, United States Code, Section 24(b).

25. Medicare is administered by the Centers for Medicare and Medicaid Services (“CMS”), which is an agency of the Department of Health and Human Services (“HHS”).

26. Medicare is subdivided into multiple program “parts.” Medicare Part A covers health care services provided by hospitals, skilled nursing facilities, hospices, and home health agencies. Medicare Part B covers physician and other licensed provider services and outpatient care, including an individual’s access to durable medical equipment (“DME”).

27. DME includes orthotic devices, such as knee braces, back braces, shoulder braces, wrist braces, and other devices. Under Medicare Part B, beneficiaries only receive Medicare-covered DME from “suppliers” that are enrolled in Medicare.

28. DME is equipment designed for repeated use and for a medical purpose, such as orthotic devices (including back, arm, and knee braces), wheelchairs, prosthetic limbs, collagen dressing, gauze, and hydrocolloid dressing.

29. Medicare reimburses DME companies for items and services rendered to beneficiaries. To receive payment from Medicare, providers must submit or cause the submission of claims to Medicare.

30. To enroll in Medicare Part B, DME suppliers are required to submit a completed enrollment also known as the “Form CMS-855S” to Medicare. The Form CMS-855S lists many standards necessary to obtain and retain Medicare billing privileges as a DME supplier.

31. The Form CMS-855S requires applicants to disclose to Medicare any individual or organization with an ownership interest, a financial interest, or managing control of a DME supplier. This includes anyone with 5% or more of an ownership stake, either direct or indirect, in

the DME supplier; anyone with a partnership interest in the DME supplier, regardless of the percentage of ownership, any organizations with “managing control” over the DME supplier, as well as any and all “managing employees.”

32. The form also requires the signature of an “authorized official” who certifies, among other things, that the DME supplier will abide by all Medicare laws, regulations, and instructions and not knowingly present or cause to be presented a false or fraudulent claim for payment by Medicare and will not submit claims with deliberate ignorance or reckless disregard of their truth or falsity.

33. A Medicare claim for DME reimbursement is required to set forth, among other things, the beneficiary’s name and unique Medicare identification number, the equipment provided to the beneficiary, the date the equipment was provided, the cost of the equipment, and the name and unique physician or provider identification number of the provider who prescribed or ordered the equipment.

34. Medicare reimburses claims for DME only if the DME was medically necessary for the treatment of the beneficiary’s illness or injury, prescribed by an appropriate medical provider, and actually provided to the beneficiary as billed.

35. The proper process involves examination of the patient by a physician or other appropriate licensed medical provider. After the examination, the provider is supposed to write a prescription for the beneficiary. The prescription should contain the patient’s identifying information, the DME item that the treating provider believes is medically necessary for the patient, and the diagnosis codes relating to the patient’s medical condition. Absent a valid

certification by the treating physician/provider, Medicare lacks the statutory authority to pay the claim.¹

36. The prescription is then provided to the DME company, which provides the necessary equipment to the patient and submits a claim directly to Medicare for reimbursement.

37. The Healthcare Common Procedure Coding System (“HCPCS” codes) are published by the American Medical Association. The codes are part of a uniform coding system used to identify, describe, and code medical, surgical, and diagnostic services performed by practicing physicians and other healthcare providers. DME suppliers use HCPCS codes to identify, describe, and code equipment and materials that they supply. These codes are used to determine the reimbursement.

B. The Relevant Parties

38. Dune Medical Supply, LLC (“Dune”) is a North Carolina corporation located at 2310 North Centennial Street, Suite 102 High Point, NC 27265, that purportedly provides DME to Medicare beneficiaries.

39. Prospect Health Solutions, Inc (“Prospect”) is a Florida corporation located at 5460 North State Road 7, Fort Lauderdale, FL 33319, that purportedly provides DME to Medicare beneficiaries.

40. Chaudhry Ahmed was a resident of Guilford County and is the owner and registered agent of Dune and the owner and registered agent of Prospect. According to Medicare enrollment documents, Ahmed is listed on the Form CMS-855S as the owner of both Dune and Prospect.

¹ See 42 U.S.C. §§ 1395n(a)(2)(b) and 1395y(a)(1) (“No payment may be made...for any expenses incurred for items or services...which...are not reasonable and necessary for the diagnosis or treatment of illness or injury...”).

Ahmed electronically signed the document and agreed that he would not present, or cause to be presented, any false or fraudulent claim for payment to Medicare.

C. The Scheme

41. From on or about April 27, 2024, through present, Medicare received complaints from hundreds of beneficiaries or providers claiming that Dune was fraudulently billing Medicare for DME that the beneficiaries never received, requested, needed, or the provider never ordered. To date, over 580 complaints have been received related to Dune.

42. From on or about June 1, 2024, through present, Medicare received complaints from hundreds of beneficiaries or providers alleging that Prospect was fraudulently billing Medicare for DME that the beneficiaries never received, requested, needed, or the provider never ordered. To date, over 450 complaints have been received related to Prospect.

Claims Analysis: Dune

43. A review of Medicare claims data revealed that Dune began submitting claims to Medicare around April 2024. Then from around April 2024 through around August 19, 2024, Dune submitted more than 36,000 claims for over 20,000 Medicare beneficiaries, resulting in claims reimbursement requests of over \$56.3 million.

44. Data analysis showed that Medicare has approved disbursement of more than \$15.4 million to Dune.

45. Of the total claims Dune submitted to Medicare, more than \$54.1 million were billed to Medicare in the 60-day period ending August 19, 2024, which represented an increase of over 2,400% when compared to the previous 60 days. Based on my training and experience, I know that a significant increase in claim submission over a short period of time, as reflected in Dune's billings to Medicare, can be indicative of fraud.

46. Furthermore, analysis of claims data showed that for approximately 67% of the claims Dune submitted, the beneficiary that allegedly received DME had no prior relationship with the provider that allegedly ordered the DME. This is significant because, as explained above, a DME order must be prescribed by an appropriate licensed medical provider based on the beneficiary's underlying condition. If a medical provider has no prior relationship with the beneficiary, it indicates the provider may not be one of the beneficiary's regular medical providers as well as they may not know whether the DME equipment was medically necessary. Based on my training and experience, I know that a high percentage of claims in which there is no prior relationship between the ordering provider and the beneficiary, as reflected in Dune's billings to Medicare, can be indicative of fraud.

47. Claims data also showed that approximately 75% of the beneficiaries on whose behalf Dune billed Medicare were identified in a separate investigation indicating that their identities were compromised and used unlawfully by individuals to obtain fraudulent reimbursements from Medicare. Based on my training and experience, compromised Medicare beneficiary information is shared or exchanged between fraudsters and is often used in subsequent fraudulent claim schemes.

48. Dune also submitted claims to Medicare for more than 115 beneficiaries who were deceased prior to the date of service listed on the claim. Several of those beneficiaries died more than three years before the date of service listed on the claim.

Claims Analysis: Prospect

49. A review of Medicare claims data revealed that Prospect began submitting claims to Medicare around May 2024. Then from around May 2024 through around August 19, 2024,

Prospect submitted more than 28,000 claims for over 17,000 Medicare beneficiaries, resulting in claims reimbursement requests of over \$45.6 million.

50. Data analysis showed that Medicare has approved disbursement of more than \$17.8 million to Prospect.

51. Of the total claims Prospect submitted to Medicare, more than \$45.1 million were billed to Medicare in the 60-day period ending August 19, 2024, which represented an increase of over 8,600% when compared to the previous 60 days.

52. Furthermore, analysis of claims data showed that for approximately 70% of the claims Prospect submitted, the beneficiary that allegedly received DME had no prior relationship with the provider that allegedly ordered the DME. The significance of this is explained in paragraph 46.

53. Claims data also showed that approximately 77% of the beneficiaries on whose behalf Prospect billed Medicare were identified in a separate investigation indicating that their identities were compromised and used unlawfully by individuals to obtain fraudulent reimbursements from Medicare.

54. Prospect also submitted claims to Medicare for more than 50 beneficiaries who were deceased prior to the date of service listed on the claim. Several of those beneficiaries died more than three years before the date of service listed on the claim.

55. According to data analysis, Prospect submitted claims to Medicare for DME for at least 24 beneficiaries from Greensboro, North Carolina.

Sample Interviews of Beneficiaries

56. Investigators interviewed numerous beneficiaries who submitted complaints to Medicare/HHS. For example, in or around July 2024, Dune submitted claims totaling

approximately \$1,963 to Medicare for a customized back brace (HCPCS L0637) purportedly provided to beneficiary D.U.

57. Law enforcement officers interviewed K.G., daughter of Medicare beneficiary D.U. K.G. advised her mother, who resides in an assisted living facility, received a box containing a back brace. The box also contained documents which referenced Medicare would pay for it. D.U. informed K.G. that she did not order the brace. K.G. noted D.U. has suffered chronic back pain for a long time but does not do anything to treat it other than aspirin. K.G. provided photos of the brace, packaging, and documentation.

58. Similarly, around August 2024, Dune submitted claims totaling approximately \$1,715 to Medicare for a back brace (HCPCS L0651) purportedly provided to beneficiary K.D.

59. Law enforcement officers interviewed K.D. who confirmed she previously submitted a complaint regarding Dune Medical Supply. According to K.D., she received a box with no return label which contained a back brace. K.D. was not aware she was going to receive this brace because she does not have any problems with her back. She did not order the brace and believes her doctor would have called her if he had ordered it for her. K.D. attempted to contact Dune on two occasions. She left messages which were not returned.

60. Claims data revealed in or around July 2024, Dune submitted claims totaling approximately \$4,397 to Medicare for a back brace and knee braces (HCPCS L0651, L2397, L1852) for Medicare beneficiary T.P.

61. Law enforcement officers interviewed T.P. T.P. stated that he received a package that contained an invoice and several back and leg braces that he had not requested. T.P. stated that he contacted his physician regarding these braces, and his doctor's nurse confirmed there had been no order for these braces from their office. T.P. stated that he called a company in High Point

about returning the braces, and he was told that they had a piece of paper with his doctor's signature on it. The employee at this company told T.P. not to worry, as the braces had already been paid for and there would be no expense to him. T.P. stated that there were two companies involved in the shipment of the braces and the company in High Point was not the same as the company listed on the package.

62. Medicare claims data also revealed in or around June 2024, beneficiary S.L. received a back brace and knee braces totaling approximately \$4,397 (HCPCS L0651, L2397, L1852).

63. Law enforcement officers interviewed the alleged prescribing physician, Dr. S.P. Dr. S.P. confirmed she was informed by patient S.L. they had received a back brace and knee braces. Dr. S.P. advised she did not order the braces and the patient does not have any medical problems which would necessitate a back brace or knee braces. Dr. S.P. does not recall receiving any phone calls or faxes asking her to sign an order for these items. Dr. S.P. noted she does not generally order braces as part of her practice.

64. Several Medicare beneficiaries for whom Prospect submitted DME claims reported in complaints to Medicare that the fraudulent DME packages they received showed that the package was shipped from Greensboro, North Carolina.

FINANCIAL ANALYSIS AND SUMMARY OF MONEY LAUNDERING ACTIVITY

65. Investigators have obtained and reviewed information related to bank accounts in the name of Dune, Prospect, and Ahmed. Only those accounts significant to this Affidavit are discussed below.

Truist Account 0067

66. Truist Bank account number 1340024270067 (Truist 0067) is a Simple Business Checking account in the name of Dune Medical Supply LLC. Investigation and bank records have shown that Ahmed has access to this account.

67. Medicare records show that Dune directed its claim reimbursements to Truist 0067, and that Medicare electronically deposits claim reimbursements to this account.

68. Records for Truist 0067 show that between May 7, 2024, and July 30, 2024, Medicare deposited approximately \$3,817,970 of claims reimbursement for DME into Truist 0067. Medicare reimbursements account for approximately 93% of the deposits and other credits to Truist 0067.

69. From August 2 to August 29, 2024 Medicare data shows an additional \$11,619,577.80 was deposited, making the total Medicare deposits for Dune Truist 0067 account \$15,437,547.94

70. On August 23, 2024, investigators obtained and served a seizure warrant issued by the United States District Court for the Middle District of North Carolina for all funds on deposit, up to \$13.6 million, in Truist 0067. (1:24MJ322-1). On or about September 9, 2024 the FBI received a check from Truist in the amount of \$5,983,084.58 in response to the seizure warrant. Investigators have determined there are no other funds remaining in this account.

JPMorgan Chase Bank Account 5016

71. JPMorgan Chase Bank account number 925915016 (Chase 5016) is a Simple Business Checking account in the name of Prospect Health Solutions Inc. Bank records show that Ahmed has access to this account.

72. Medicare records show that Prospect Health Solutions directed its claim reimbursements to Chase 5016, and that Medicare electronically deposits claim reimbursements to this account.

73. Through July 31, 2024, Medicare reimbursements accounted for more than 98% of the deposits and other credits to Chase 5016. Between June 4, 2024, and August 21, 2024, Medicare deposited approximately \$8.9 million of claims reimbursement for DME into Chase 5016. Based on Medicare data, Medicare also deposited approximately \$8.9 million into Chase 5016 from August 22 through August 30, 2024.

74. On August 23, 2024, investigators obtained and served a seizure warrant issued by the United States District Court for the Middle District of North Carolina for all funds on deposit, up to \$8.9 million, in Chase 5016. (1:24MJ321-1). On or about September 10, 2024 the FBI received a check from Chase in the amount of \$8.9 million in response to the seizure warrant.

Pinnacle Bank Account 4775

75. Pinnacle Bank account number 800109474775 (Pinnacle 4775) is a checking account in the name of Prospect Health Solutions Inc. opened on or about July 24, 2024. Bank records show that Ahmed is signatory on this account.

76. Bank records for Chase 5016 show that between July 29, 2024, and August 14, 2024, \$1,363,000 was transferred from Chase 5016 into Pinnacle 4775.

Bank of America Account 3805

77. Bank of America, N.A. Account Number 237049893805 (BOA 3805) is an account in the name of Chaudhry Ahmed.

78. Investigation to date has identified approximately 30 wire transfers out of the Prospect Chase account 5016 since June 2024. These wire transfers include five transfers to the BOA 3805 account totaling \$1.5 million on or about the following dates: August 15, 2024 (\$250,000), August 19, 2024 (\$150,000), August 20, 2024 (\$300,000), August 21, 2024 (\$450,000), and August 22, 2024 (\$350,000). A cashier's check from Chase 5016 in the amount of \$150,000 was also deposited into BOA 3805 on or about July 29, 2024.

79. In addition, bank records show a wire transfer from Truist 0067 on or about August 8, 2024 (\$300,000) and two wire transfers from Pinnacle 4775 on or about August 12, 2024 (\$300,000) and August 19, 2024 (\$309,988) into BOA 3805.

80. On August 23, 2024, investigators obtained and served a seizure warrant issued by the United States District Court for the Middle District of North Carolina for all funds on deposit, up to \$750,000, in BOA 3805. (1:24MJ320-1). On September 9, 2024 the FBI received a check from BOA in the amount of \$537,111.23 in response to the seizure warrant for BOA 3805.

81. The review of the bank records for BOA 3805 also showed that approximately \$1.88 million was transferred to Coinbase account number 301188475943 held at Cross River Bank from August 5, 2024 through August 22, 2024 through a series of eight wire transfers as detailed in paragraph 83 below.

82. On or about July 20, 2024, a \$1,000 transfer was made via Zelle from BOA 3805 to Pinnacle Bank account number 800109141127, a personal checking account owned by Chaudhry Ahmed. This money was used to fund an ACH transfer to Coinbase for \$1,000 on the same day.

Coinbase

83. Coinbase, Inc. produced records for User ID 668451c92271291e4d6b5527, associated with Chaudhry Ahmed. The account was created on July 2, 2024, at 3:15pm EDT. The following fiat currency deposits were made into the account (all times denoted in Eastern Daylight Time):

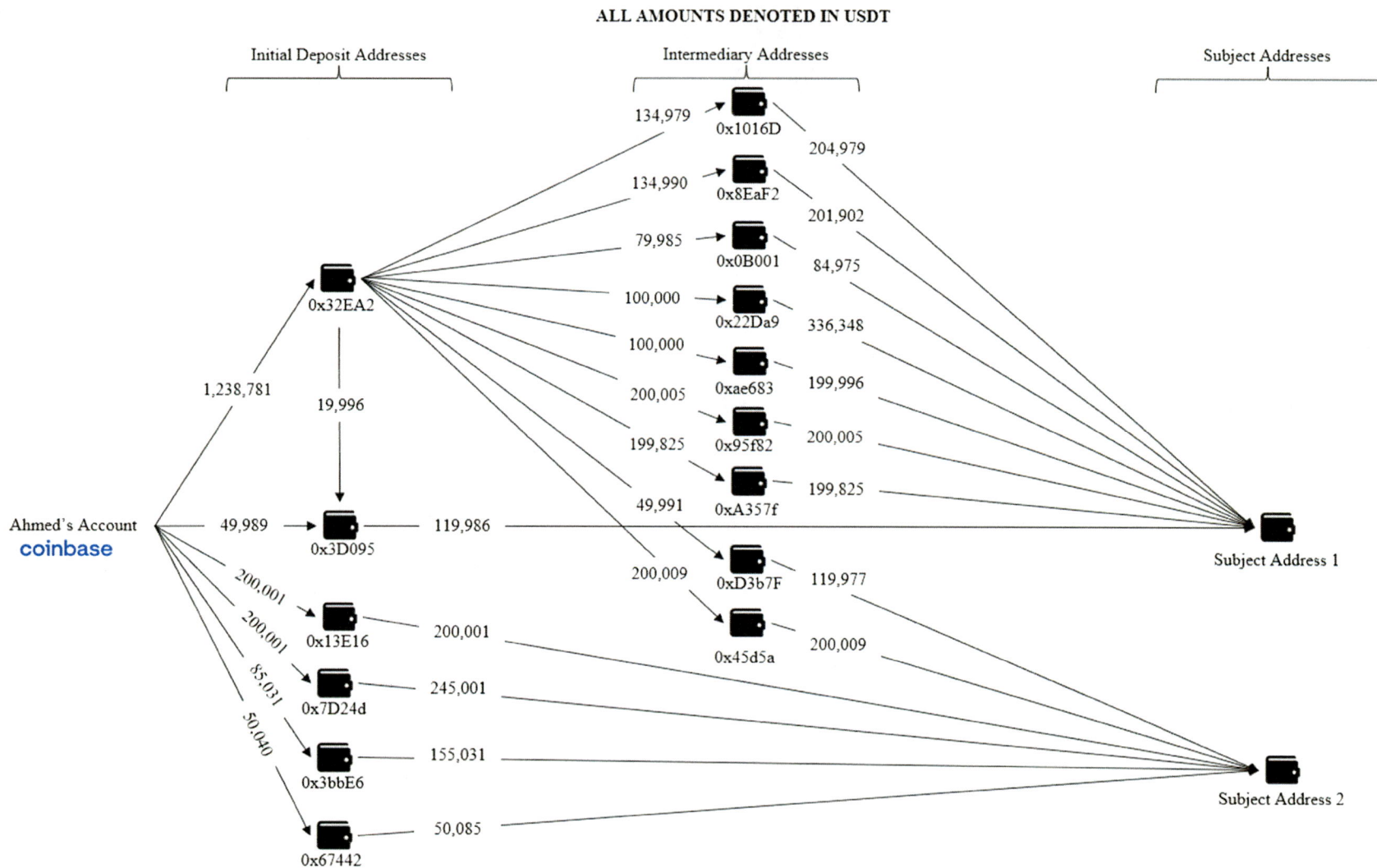
DATE & TIME	AMOUNT	FROM ACCOUNT
7/20/2024 8:34pm	\$1,000.00	Pinnacle 1127
8/6/2024 12:45pm	\$99,990.00	BOA 3805
8/8/2024 2:24pm	\$99,990.00	BOA 3805
8/9/2024 11:04am	\$279,990.00	BOA 3805
8/13/2024 3:44pm	\$249,990.00	BOA 3805
8/19/2024 1:12pm	\$299,990.00	BOA 3805
8/20/2024 5:44pm	\$299,990.00	BOA 3805
8/22/2024 9:16am	\$199,990.00	BOA 3805
8/22/2024 4:17pm	\$349,990.00	BOA 3805
TOTAL	\$1,880,920.00	

84. The fiat currency transferred to Coinbase funded the purchase of virtual currency, primarily USDT, which was subsequently sent to various virtual currency addresses used to receive and launder the funds. Between August 6, 2024, at 2:18pm and August 23, 2024, at 9:29pm EDT a total of 17 transactions² were sent to six initial deposit addresses. These six addresses received an aggregate amount of 1,823,843 USDT from Ahmed's Coinbase account (USDT amounts here and elsewhere rounded to the nearest whole value). From these six addresses, some of the USDT was sent directly to **Subject Addresses 1 and 2**, while some of the USDT moved through additional intermediary addresses before being sent to **Subject Addresses 1 and 2**. The

² Ahmed was arrested on August 23, 2024, at approximately 6:00pm EDT. Based on the timing of funds leaving Ahmed's Coinbase account, the records indicate that 3 transactions (of the 17 transactions mentioned above) occurred after Ahmed's arrest.

flow of funds from Ahmed's Coinbase account to **Subject Addresses 1 and 2** is illustrated below,³ with all amounts denoted in USDT. Arrows utilized in illustrating the flow of funds between addresses may be representative of multiple transactions. The virtual currency addresses here and elsewhere in this affidavit are truncated for ease of reference.

³The illustration is not intended to illustrate transactions that (1) went to addresses that are not subject to seizure, or (2) transactions that did not contain any funds derived from Ahmed's Coinbase account.



85. The six addresses which received the USDT directly from Ahmed's Coinbase account are depicted in the first column as "Initial Deposit Addresses." The "Intermediary Addresses," through which funds from 0x32EA2 were moved, are depicted in the second column. The "**Subject Addresses**" are depicted in the third column.

Address 0x32EA2:

86. Between August 12, 2024, at 12:11pm EDT and August 23, 2024, at 9:30pm EDT, address 0x32EA2 received 8 deposits totaling 1,238,781 USDT, all of which were sent from Ahmed's Coinbase account. Between August 12, 2024, at 12:16pm EDT and August 23, 2024, at 9:40pm EDT, address 0x32EA2 sent 12 transactions totaling 1,219,780 USDT to nine additional intermediary addresses and to 0x3D095. The funds were subsequently sent to **Subject Addresses 1 and 2.**⁴ The balance of funds in the Initial Deposit Addresses and Intermediary Addresses never fell below the deposit amounts identified in the chart prior to the transfers to the **Subject Addresses**.

87. Whether transferring BTC or, in this case, USDT on the Ethereum blockchain, each individual virtual currency transfer costs money. For USDT, that cost comes through the payment of "gas" fees required by the Ethereum blockchain.⁵ It is reasonable to assume that legitimate businesses and individuals would strive to minimize those fees by conducting transfers with as few

⁴ Certain initial deposit addresses received deposits from other sending addresses as well as from Ahmed's Coinbase. As a result, the amount sent from certain initial deposit addresses to the Subject Addresses was greater than the amount received directly from Ahmed's Coinbase. Similarly, certain intermediary addresses received deposits from other sending addresses as well as from 0x32EA2. As a result, the amount sent from certain intermediary addresses to the Subject Addresses was greater than the amount received directly from 0x32EA2.

⁵ Fees are a cornerstone of blockchain technology, as they are the rewards provided to those providing the computing power to operate the blockchain itself.

transactions, or “hops,” as possible. In the flow of funds illustrated above, the transfers through initial deposit addresses and intermediary addresses resulted in a less direct flow of funds to the Subject Addresses and the incurrence of fees, which may not have served a legitimate business or economic purpose.

88. Based upon my training and experience, and conversations with other law enforcement personnel, I know that the funneling of funds such as depicted in the diagram above is a common method used by individuals who are attempting to launder large amounts of cryptocurrency, and, therefore, want to thwart law enforcement’s ability to trace, and ultimately recover, criminal proceeds.

89. In addition, there is no apparent reason, economic or otherwise, for the use of such a complex movement of cryptocurrency through the use of multiple intermediary wallet addresses, unless the purpose is to conceal the nature, source, location, ownership or control of the funds at issue.

Subject Addresses:

90. **Subject Address 1** received 10 deposits totaling 1,643,023 USDT.⁶ All of the deposits were received between 8:42pm EDT and 10:17pm EDT on August 30, 2024, and no withdrawals have been made from this address. The FBI calculated approximately 1,019,769 USDT or approximately 62% of the total balance of **Subject Address 1** was derived from Ahmed’s Coinbase account.

⁶ For both **Subject Addresses**, the total deposits received includes deposits which are not depicted in the illustration above. Certain deposits were not depicted in the illustration because they did not contain funds traceable to Ahmed’s Coinbase account.

91. **Subject Address 2** received 9 deposits totaling 1,234,593 USDT. All of the deposits were received between 11:30pm EDT on August 30, 2024 and 1:21am EDT on August 31, 2024, and no withdrawals have been made from this address. The FBI calculated approximately 785,073 USDT or approximately 64% of the total balance of **Subject Address 2** was derived from Ahmed's Coinbase account.

SEIZURE PROCEDURE FOR THE TARGET PROPERTY

92. The foregoing establishes probable cause to believe that the **Subject Addresses** are subject to civil and criminal forfeiture, as they are proceeds of health care fraud and are involved in money laundering using virtual currency.

93. Should this seizure warrant be granted, law enforcement intends to work with Tether to seize the funds associated with the Target Property. In sum, the accompanying warrant would be transmitted to Tether, at which time Tether would "burn" (*i.e.*, destroy) the addresses at issue (and by extension the USDT tokens associated with them.) Tether would then reissue the equivalent amount of USDT tokens associated with the Target Property and transfer that equivalent amount of USDT to a government-controlled wallet. The seized currency will remain in the custody of the U.S. government during the entire pendency of the forfeiture proceedings, to ensure that access to, or manipulation of, the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

94. On September 10, 2024, the FBI requested that Tether voluntarily freeze the USDT remaining in the **Subject Addresses**. On September 12, 2024, Tether confirmed that the **Subject**

Addresses had been frozen. **Subject Addresses 1 and 2** maintained the following balances as of October 2, 2024:

ADDRESS	BALANCE
Subject Address 1	1,643,023 USDT
Subject Address 2	1,234,593 USDT
TOTAL	2,877,616 USDT

CONCLUSION

95. Based on information derived from the foregoing investigation, there is probable cause to conclude that the **Subject Addresses** received the proceeds of a health care fraud scheme and money laundering scheme performed in violation of 18 U.S.C. § 1347 (health care fraud), and 18 U.S.C. § 1956(a)(1)(B)(i) and 18 U.S.C. § 1957, and 18 U.S.C. § 1956(h) (money laundering and violation of the spending statute). Those proceeds are subject to forfeiture as proceeds of health care fraud, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), and as property involved in money laundering offenses, pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1). Accordingly, I respectfully request that warrants be issued authorizing the seizure of the **Subject Funds**.

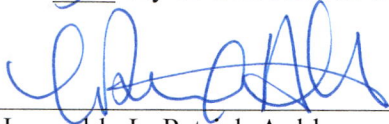
96. Based on the foregoing, I request that the Court issue the proposed seizure warrants. Because the warrants will be served on Tether, who will then collect the funds at a time convenient to it and wire it to the government, there exists reasonable cause to permit the execution of the requested warrants at any time in the day or night.

This the 3rd day of October 2024.

/s/ David Yu
David Yu
Special Agent
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Applicant appeared before me by telephone, was placed under oath, and attested to the contents of this Application, which was submitted to me by reliable electronic means.

This 30th day of October 2024.



Honorable L. Patrick Auld
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A: PROPERTY TO BE SEIZED

Pursuant to this warrant, Tether shall provide the law enforcement officer/agency serving this document with the equivalent amount of USDT tokens that are currently associated with the virtual currency addresses referenced below (*i.e.*, 2,877,616 USDT). Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency wallet. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

- All Tether (“USDT”) held in address

0xFa05456F82a0B816CD1dc1e9233BE75908fCd9b8 (“Subject Address 1”)

- All Tether (“USDT”) held in address

0xD4C06e5554a2c4F18269126Cc5d530dd1D43dC4E (“Subject Address 2”)